

DETAILED ACTION

1. Claims 1-27 are pending.
2. Claims 1, 22, and 27 are amended.

Response to Arguments

4. Applicant's arguments filed with respect to claims 1-27 have been fully considered but they are not persuasive.

On page 11 of the applicant's response, the applicant argues that Kunzinger fails to teach or suggest the direct exchange of keys between the client and the server, and that Kunzinger teaches away from the first computer and second computer negotiating and exchanging keys with one another.

The examiner respectfully disagrees. Kunzinger teaches a security method between two end points, and does not teach away from direct communication but in fact teaches an embodiment where direct negotiation occurs. Kunzinger, [0072], teaches that the cascade enabled flag may not be set. When the flag is not set then the system uses prior art methods of secure connection. Prior art methods have the two endpoints negotiate keys with one another [0007] L1-9 and [0014] L1-2 and [0017] L1-3. The negotiation is direct with one another, and each endpoint is equivalent to the first computer and the second computer. Therefore Kunzinger does teach the argued limitations and does not teach away from the claimed invention.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2, 4-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Kunzinger (Pub No: 2002/0091921).

As to claim 1, Kunzinger teaches a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network (Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising: the first computer and the second computer negotiating and exchanging keys with one another (Kunzinger, [0072] the cascade enabled flag can not be set and prior art negotiation of keys directly takes place [0007] L1-9 and [0014] L1-2 and [0017] L1-3) according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer (Kunzinger, [0067] and [0068], the client establishes a secure connection to the endpoint using the IPSec and internet key exchange policy since the endpoint is within and intranet a gateway is an intermediary), the secure connection having a source address of the first computer as a first end point

and a destination address of the second computer as a second end point of the secure connection (Kunzinger, [0013], the IPSec packet has an inner header with the source and destination addresses), in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer, (Kunzinger, [0068] L1-3, the key is the id and [0013] the outer header has the address of the endpoint of the tunnel, i.e. gateway), sending the secure message from the first computer to the intermediate computer, the intermediate computer receiving the secure message (Kunzinger, [0068] L1-3, the message is sent from the client and received by the gateway) and performing a translation by using the first unique identity to find a second destination address to the second computer , the intermediate computer substituting the first destination address with the second destination address to the second computer, the intermediate computer substituting the first unique identity with a second unique identity of the secure connection (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer), and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

As to claim 2, Kunzinger teaches wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer (Kunzinger, [0067], IPSec protection).

As to claim 4, Kunzinger teaches wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection (Kunzinger, [0067], IKE is used to for the IPSec connection).

As to claim 5, Kunzinger teaches wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol (Kunzinger, [0067], IKE is used to for the IPSec connection).

As to claim 6, Kunzinger teaches wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically) and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer (Kunzinger, [0069] using IKE between gateway and server).

As to claim 7, Kunzinger teaches wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer,

the unique identity (Kunzinger, [0013], inner and outer headers and negotiated security association).

As to claim 8, Kunzinger teaches wherein the method further comprises the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values (Kunzinger, [0067], setting up the IPSec SA and the values are SPI values).

As to claim 9, Kunzinger teaches wherein the method further comprises performing the matching by using a translation table stored at the intermediate computer (Kunzinger, [0066], the databases are the translation tables).

As to claim 10, Kunzinger teaches wherein the method further comprises changing both the address and the SPI-value by the intermediate computer (Kunzinger, [0074], the address is changed to point to the tunnel and the ID(SPI) is changed, the SPI is the ID that is exchanged for indexing).

As to claim 11, Kunzinger teaches wherein the method further comprises the first computer being a mobile terminal (Kunzinger, [0038], the workstations communicate over a wireless cellular network) so that the mobility is enabled by modifying the translation table at the intermediate computer (Kunzinger, [0067] L13-17, the SAD on the gateway is modified with IKE value).

As to claim 12, Kunzinger teaches wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new

address from the first computer to the intermediate computer (Kunzinger, [0062], the client is the IKE initiator with negotiations with the gateway).

As to claim 13, Kunzinger teaches wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer (Kunzinger, [0063], the gateway is the IKE responder to the client in the IKE negotiations).

As to claim 14, Kunzinger teaches wherein the method further comprises authenticating or encrypting by IPSec the request for registration and/or reply (Kunzinger, [0067], authenticating IPSec).

As to claim 15, Kunzinger teaches wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).

As to claim 16, Kunzinger teaches wherein the method further comprises establishing the key exchange distribution by: generating an initiator cookie and sending a zero responder cookie to the second computer, generating a responder cookie in the second computer (Kunzinger, [0064] [0065] and [0067], the gateway is the initiator and the server is the responder in the IKE negotiations. [0069] shows an example of IKE negotiations the IDCi and IDCr values are set), establishing a mapping between IP

addresses and IKE cookie values in the intermediate computer, and using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).

As to claim 17, Kunzinger teaches wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).

As to claim 18, Kunzinger teaches wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).

As to claim 19, Kunzinger teaches wherein the method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table (Kunzinger [0074] the gateway uses

tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).

As to claim 20, Kunzinger teaches wherein the method further comprises sending the secure message by using an IPSec transport mode (Kunzinger, [0075] L12-15, IPSec operates in transport mode).

As to claim 21, Kunzinger teaches wherein the method further comprises sending the secure message by using an IPSec tunnel mode (Kunzinger, [0075] L12-15, IPSec operates in tunnel mode).

As to claim 22, Kunzinger teaches a telecommunication network for secure forwarding of messages (Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising: a first computer, a second computer and an intermediate computer, means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (Kunzinger, [0072] the cascade enabled flag can not be set and prior art negotiation of keys directly takes place [0007] L1-9 and [0014] L1-2 and [0017] L1-3), the first and the second computers having means for performing an IPSec processing, the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a

secure message to a destination address of the second computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel (IKE/IPSec) and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer), and the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the security association (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

As to claim 23, Kunzinger teaches wherein the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).

As to claim 24, Kunzinger teaches wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer (Kunzinger, [0066] L1-10, each set of interfaces has its own databases).

As to claim 25, Kunzinger teaches wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address (Kunzinger, [0067] IKE tables have the addresses for endpoint association), initiator and

responder cookies between respective computers (Kunzinger, [0067], IDci and IDcr values).

As to claim 26, Kunzinger teaches wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer (Kunzinger, [0066], association for a user to an endpoint).

As to claim 27, Kunzinger teaches a telecommunication network for secure forwarding of messages (Kunzinger, [0047] L 1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising: a first computer, a second computer, an intermediate computer electronically connected to the first computer and the second computer, means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (Kunzinger, [0072] the cascade enabled flag can not be set and prior art negotiation of keys directly takes place [0007] L 1-9 and [0014] L 1-2 and [0017] L 1-3), and the intermediate computer having means for performing translation between destination addresses and secure identities (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer) for forwarding secure messages received from the first computer to the second computer in the secure connection (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzinger as applied to claim 1 above, and further in view of Patel (Pub No: 2002/0004900).

As to claim 3, Kunzinger teaches the limitations of claim 1. Kunzinger does not teach wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols. Patel teaches wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols (*Patel, [0037] L18-21, SSL for secure connection*). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Kunzinger with Patel to use SSL for the secure connection because Patel teaches that SSL is a well known protocol for a secure connection that can be used like IPsec.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AFSHAWN TOWFIGHI whose telephone number is (571)270-7296. The examiner can normally be reached on Monday - Friday 9:00 A.M. to 6:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ian Moore can be reached on (571)272-3085. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/A. T./
Examiner, Art Unit 2469

/Ian N. Moore/
Supervisory Patent Examiner, Art Unit 2469